VERSAL TORSORS WITH FEW PARAMETERS

GOMBODORJ BAYARMAGNAI

Abstract. We introduce certain versal torsors corresponding to twisted cyclic groups of order at least three and study their properties, particularly the number of required parameters. In particular, we attach to the cyclic group C_n a monic polynomial of degree n under certain condition on the base field.

In the context of all cyclic extensions over an arbitrary field extension of the base field, we establish various generic properties for our polynomials and further give a family of generic Galois cyclic extensions in terms of our polynomials.

1. Introduction

Let k be a field and G be a smooth affine algebraic group scheme over k. Then it is a fundamental problem to determine minimal elements among all versal G-torsors in the sense of Serre [5]. Here the minimality is measured by the essential dimension of G over k which is a numerical invariant introduced by Buhler-Reichstein in [2] and Reichstein in [15], and generalized by Merkurjev in [3]. In the paper we restrict our attention to the case of twisted cyclic groups G over k. Then it is natural to ask what are the extensions with G-structure that correspond to the minimal versal G-torsors. On the other side, for finite groups G, we also have the following important notions originated by Saltman; namely, generic polynomials of G over k and generic Galois extensions for G over k. In the context of all G-extensions over an arbitrary field extension of k, a generic polynomial for the pair (G, k) (if it exists) generates all field extensions with Galois group G, while a versal G-torsor controls all Galois G-algebras. The essential dimension determines the number of required parameters needed for versal G-torsors and the generic dimension counts the minimal number of parameters of generic polynomials. In fact, it is expected that both dimensions are equal for any finite group and field; see Berhuy-Favi [3], Jensen-Ledet-Yui [6], Malle-Matzat [13] and Saltman [19] for more information.

For example, by classical Kummer theorem, the cyclic torsor corresponding to the etale k-algebra defined by $k(t)[X]/\langle P_n(t;X)\rangle$ is versal if the base field k contains a primitive n-th root of unity ζ_n and characteristic of k is prime to n. Here, t is a parameter and the polynomial $P_n(t;X)$ is given by

$$P_n(t;X) = \prod_{i=1}^{n}(X - \zeta_n^i u) \in k(t)[X],\ (u^n = t).$$

This cyclic torsor is minimal, since the essential dimension of the cyclic group of order n over k is 1. Moreover, the polynomial $P_n(t;X)$ is a generic cyclic polynomial over k and the cyclic extension $R[X]/\langle P_n(t;X)\rangle$ of R is a generic Galois extension over k in the sense of Saltman, where R stands for $k[t, 1/t]$. If we require that ζ_n is not in k, then the problem

Date: March, 2010.

becomes more complicated since the essential dimension of cyclic groups grows (see, for example, [4] and [12]).

The main object of this paper is to study a minimal torsor with respect to certain twisted cyclic group of order n and its relationship with notions discussed above. To be more precise, fix a positive integer $n \geq 3$ and let k be a field whose characteristic is prime to $2n$. Let G be a twisted k-form of μ_n coming from a quadratic extension of k (Definition 2.2). Then we have the G-torsor T defined as the fiber in the torus $Res_{K/k}\mathbb{G}_m$ at the generic point of the quotient $Res_{K/k}/G$. Indeed, it is a versal torsor because the affine algebraic k-group $Res_{K/k}/G$ classifies all G-torsors. If n is odd, one gets a versal torsor of essential dimension one (from T) by compression. The purpose of the first result of this paper is to show the minimality (in the sense of essential dimension) of the G-torsor T for even n. In the section 4, we prove Theorem 4.3 which says that

$$ed_k G = 2$$

for even $n \geq 4$. Note here that our method is motivated by that of Rost in [17] and the above is the result of [17] if n is divisible by four. In our proof, the natural invariant res defined by $res : H^1(\ , G) \to H^1(\ , Res_{K/k}\mu_n)$ plays a main role.

We expect that the study of twisted cyclic groups is a reasonable first step towards the understanding of the behavior of versal torsors for finite nonabelian groups.

The next goal of the paper is to provide a more concrete description of the torsor T (Lemma 4.1) with respect to the cyclic group C_n. The template of the results obtained in Section 5 is the following. Assume the base field k contains $\omega_n^+ = \zeta_n + \zeta_n^{-1}$. Then the C_n-torsor T is determined by the splitting field over $k(x, y)$ for the polynomial

$$P_n(\omega_n^- x, y, 1; T) = \prod_{i=1}^{n} \left(T - u\zeta_n^i - \frac{y}{u\zeta_n^i} \right) \in k(x, y)[T].$$

Here u^n is expressed in terms of some parameters x, y and, moreover, one may assume that $y = 1$ if n is odd. Surprisingly, the polynomial is a descent-generic polynomial for C_n over k. We should mention that a versal G-torsor does not produce a generic polynomial in general. Indeed, Lenstra [11] proved that the group C_n does not have a generic polynomial over $\mathbb{Q}$ if n is divisible by eight. However, even in this case, we still have versal torsors.

Under the same assumption of base field, alternative constructions of generic polynomials for cyclic groups can be found in Rikuna [16] for odd degree, in Ledet [6] and Hashimoto-Rikuna [9] for even degree. These are based on an affirmative solution for linear Noether's problem. Our method is the following:

1. We use the natural cohomological invariant $res : H^1(\ , C_n) \to H^1(\ , Res_{k(\zeta_n)/k}\mu_n)$ to deal with the generic properties for C_n-extensions over any field extension of k.

2. There are exactly two 1-dimensional tori; the multiplicative group $\mathbb{G}_m$ and the norm torus. We use these tori for a classifying space of the functor $H^1(\ , C_n)$ to compute the invariant res explicitly.

This method allows us to construct a family of generic cyclic extension of order n in terms of the polynomial $P_n((\omega_n^- x, y, z; T)$ and, moreover, one may assume that $y = 1$ if n is odd . Finally, with these two main results of the paper we conclude that the generic dimension coincides with the essential dimension for cyclic groups over the base field k.

Acknowledgements. The author would like to thank Oda Takayuki and Battsengel Baasanjav for their constant encouragement. He would also like to thank Zinovy Reichstein for some useful advice.

The present manuscript was partially completed during the visit of the author at the Hausdorff Institute of Mathematics in Bonn, during the Trimester Program on Algebra and Number Theory. The author wish to warmly thanks this institution for providing an excellent research environment.

Notations. We consider fields K over the base field k and the cyclic group C_n of order n with trivial action of Γ_k, where Γ_k denotes the absolute Galois group of k. Set $\omega_n^{\pm} = \zeta_n \pm \zeta_n^{-1}$, where ζ_n stands for a primitive nth root of unity. As usual, μ_n is the group scheme of n-th roots of unit. We let K_n denote the field $K(\zeta_n)$ if K is a proper subfield of $K(\zeta_n)$.

Let L/K be a finite and separable extension. Then $T_{L/K}$ denote the torus $Res_{L/K}(\mathbb{G}_m)$, obtained from $\mathbb{G}_m$ by Weil restriction scalars from L to K. We mean by $X(T)$ the character group of an algebraic k-torus T.

For $n \geq r \geq 0$, the symbol $\binom{n}{r}$ is the binomial coefficient. We often use $[x]$ to denote the equivalence class containing a certain element x.

2. Basic objects

In this section we introduce basic objects of our investigations and constructions.

2.1. **Polynomials.** In this subsection, for any positive integer $n \geq 3$, we construct a polynomial of degree n with coefficients in a pure transcendental extension of degree at most 3 over k. We relate it to the cyclic group of order n in the section 5 under the light of the section 3.

Proposition 2.1. *Let t_1, t_2, t_3 be algebraically independent over the field k. For every positive integer n, define a monic polynomial $P_n(t_1, t_2, t_3; X)$ of variable X by*

$$P_n(t_1, t_2, t_3; X) = \prod_{i=1}^{n} \left(X - u\zeta_n^i - \frac{t_2}{u\zeta_n^i} \right),$$

where u is a root of the polynomial $X^n - t_2^{[\frac{n}{2}]}(t_3 + t_1)(t_3 - t_1)^{-1}$. Then the coefficients of the polynomial

$$\begin{cases} P_n(t_1, t_2, t_3; X), & \text{if } n \text{ is even} \\ P_n(t_1, 1, t_3; X), & \text{if } n \text{ is odd} \end{cases}$$

belong to the field $k(t_1^2, t_2, t_3^2)$.

Proof. Let v be a variable. Then for each positive integer s, let $a_s = v^s + v^{-s}$. Then the sequence $\{a_s\}_{s=0}^{\infty}$ satisfies the recurrence relation $a_s = a_1 a_{s-1} - a_{s-2}$. By setting $Y = a_1$ and $m = [n/2]$, the member a_s can be expressed as a polynomial in Y as follows:

$$a_s = 2^{-s}\big(Y + \sqrt{Y^2 - 4}\,\big)^s + 2^{-s}\big(Y - \sqrt{Y^2 - 4}\,\big)^s = \sum_{j=0}^{m} A_j(m) Y^{s-2j} \tag{1}$$

where

$$A_j(m) = 2^{1-s}(-4)^j \sum_{i=j}^{m} \binom{s}{2i}\binom{i}{j}.$$

In order to get a polynomial with coefficients in $k(t_1,t_2,t_3)$ which has the root $u+t_2/u$, we represent $(u+t_2/u)^n$ in terms of $u+t_2/u$. Now assume that n is even, $n=2m$, for some integer m.

Observe that

$$Y^n = (v+v^{-1})^n = \sum_{i=0}^{n}\binom{n}{i}v^{2(i-m)} = a_n + \binom{n}{m} + \sum_{i=1}^{m-1}\binom{n}{i}a_{m-i}.$$

Using (1) we conclude that

$$Y^n = a_n + \binom{n}{m} + \sum_{i=1}^{m-1}\binom{n}{i}\sum_{j=0}^{m-i} A_j(m-i)Y^{2(m-i-j)} \tag{2}$$

$$= a_n + \binom{n}{m} + \sum_{h=1}^{m-1}\Big\{\sum_{i+j=h}\binom{n}{i}A_j(m-i)\Big\}Y^{2(m-h)}. \tag{3}$$

For a fixed integer $1 \le i \le n$, now we make the change in variable

$$v = u\zeta_n^i/\sqrt{t_2}$$

and write $u\zeta_n^i + t_2/u\zeta_n^i$ in the form $\sqrt{t_2}(v+v^{-1})$. With this notation, for each i, we have that

$$a_n = 2\frac{t_3^2+t_1^2}{t_3^2-t_1^2}.$$

Therefore we can conclude from (3) that each $u\zeta_n^i + t_2/u\zeta_n^i$ is a root of the polynomial in X with coefficients in $k(t_1,t_2,t_3)$ given by

$$X^n - 2^{1-n}\sum_{k=1}^{\frac{n}{2}-1} t_2^k A_k X^{n-2k} - t_2^{\frac{n}{2}}\binom{n}{n/2} - \frac{2t_2^{\frac{n}{2}}(t_1^2+t_3^2)}{t_3^2-t_1^2},$$

where

$$A_k = \sum_{i+j=k}\binom{n}{i}A_j(m-i).$$

By definition, the above is our polynomial $P_n(t_1,t_2,t_3;X)$. The odd case can be done similarly. □

Example 1. The simplest case is $n=3$ and $k=\mathbb{Q}$. Note that $\omega_3^- = \sqrt{-3}$. We have the polynomial $P_3(\omega_3^- t,1,1;X)$ in variable X expressed by

$$X^3 - 3X - 2(1-3t^2)/(1+3t^2) \in \mathbb{Q}(t)[X],$$

which is known as a generic cyclic polynomial of degree 3 over $\mathbb{Q}$:

Example 2. Assume $n=4$. Consider the following polynomial in variable X:

$$P_4(\sqrt{-1}t_1,t_2,1;X) = X^4 - 4t_2X^2 + 4t_2^2t_1^2/(1+t_1^2).$$

Letting $t_1 \to t$ and $t_2 \to s(1+t^2)/2$, we get a polynomial

$$X^4 - 2s(1+t^2)X^2 + s^2t^2(1+t^2) \in k(s,t)[X].$$

It is well known example as a generic cyclic polynomial over a field of characteristic not 2.

2.2. **Twisted groups.** The book [8], by Knus-Merkurjev-Rost-Tignol, will be our main reference for this subsection and the next section. Fix a positive integer $n \geq 3$ and let k be a filed of characteristic prime to $2n$. Let

$$\mu_n = Spec(k[x]/(x^n - 1))$$

denote the k-group of the n-th roots of the unity. Since the conjugation action of $\mathrm{Gal}(k_s/k)$ on $Aut(\mu_n)$ is trivial, we have

$$H^1(k, Aut(\mu_n)) \cong \mathrm{Hom}(\Gamma_k, (\mathbb{Z}/n\mathbb{Z})^\times).$$

The left hand side classifies isomorphism classes of twisted k-forms of μ_n. For every quadratic extension K/k we define a homomorphism $f_K : \mathrm{Gal}(K/k) \to Aut(\mu_n)$ by sending the nontrivial element to the inverse automorphism $\zeta_n \to \zeta_n^{-1}$.

Definition 2.2. *Let G be a twisted k-form G of μ_n attached to the homomorphism $\Gamma_k \to Aut(\mu_n)$ that factors through f_K for some quadratic extension K/k. In this case, we call G a twisted group of μ_n coming from the quadratic extension K/k.*

More precisely, the homomorphism corresponding to G is a composition of the natural homomorphism $\Gamma_k \to \mathrm{Gal}(K/k)$ with f_K defined above.

Example. We assume that the base field k contains ω_n^+ but does not ζ_n. Then the cyclic group C_n is the twisted k-form of μ_n coming from the quadratic extension k_n/k.

For any field extension L/k one has that $T_{K/k}(L) \cong (K \otimes_k L)^\times$. Therefore we may assume that any element of $T_{K/k}(L)$ can be written in the form

$$1 \otimes x + \sqrt{a} \otimes y \quad \text{with } x, y \in L$$

by setting $K = k(\sqrt{a})$. The norm map $N_{K/k}$ sends it to $x^2 - ay^2$. Let $g_\pm$ denote the element

$$1 \otimes \frac{\omega_n^+}{2} \pm \sqrt{a} \otimes \frac{\omega_n^-}{2\sqrt{a}}$$

in $(K \otimes_k \bar{k})^\times$.

Lemma 2.3. *Let G be a twisted group coming from a quadratic extension K/k. The group G can be identified with a cyclic group generated by the element g_+ with the inverse g_-.*

Proof. For any positive integer m one has that

$$g_+^m = 1 \otimes \frac{\zeta_n^m + \zeta_n^{-m}}{2} + \sqrt{a} \otimes \frac{\zeta_n^m - \zeta_n^{-m}}{2\sqrt{a}}.$$

by induction on m. Hence, the order of g_+ is exactly n and further one can easily verify the coincidence of Γ_k-action, because the action of Γ_k on G is determined by the action $\mathrm{Gal}(K_n/k)$. □

2.3. **Versal G-torsors.** We follow the definition of versal torsor introduced in [5] and also refer the reader to [3], [15] and [17]. A simple example of a versal torsor with respect to cyclic group is the μ_n-torsor $[n] : \mathbb{G}_m \to \mathbb{G}_m$, where $[n]$ is the n-power map.

We keep notations in the previous subsection. The character module $X(T_{K/k})$ of $T_{K/k}$ is isomorphic to the Γ_k-module $\mathbb{Z}[x]/\langle x^2 - 1\rangle$, where the action of Γ_k is identified with multiplication by x. It is clear that the canonical comorphism $\mathbb{Z}[x]/\langle x - 1\rangle \to X(T_{K/k})$

corresponds to the norm map $N_{K/k} : T_{K/k} \to \mathbb{G}_m$. Now we can restate Lemma 2.3 as follows.

Lemma 2.4. *Let G be a twisted k-group coming from a quadratic extension K/k. Then it is isomorphic to the kernel of the norm map $N_{K/k}$ from $Res_{K/k}(\mu_n)$ to the group μ_n.*

We can deduce that $\phi : T_{K/k} \to T_{K/k}/G$ is a versal G-torsor since the first Galois cohomology vanishes for $T_{K/k}$. Denote by $T^{(1)}_{K/k}$ the kernel of $N_{K/k}$. Then one has that $X(T^{(1)}_{K/k}) \cong \mathbb{Z}[x]/\langle x+1\rangle$ as Γ_k-modules. The canonical comorphism from $X(T^{(1)}_{K/k})$ to $X(T_{K/k})$ defines a morphism from $T_{K/k}$ onto $T^{(1)}_{K/k}$, denote it by $\Delta_{K/k}$. Lemma 2.4 gives us a Kummer type exact sequence for G:

$$1 \to G \to T^{(1)}_{K/k}(\bar{k}) \xrightarrow{[n]} T^{(1)}_{K/k}(\bar{k}) \to 1, \tag{4}$$

where $[n]$ is the n-power map. Moreover, we have the following commutative diagram:

$$\begin{array}{ccc} T_{K/k} & \xrightarrow{\Delta_{K/k}} & T^{(1)}_{K/k} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle[n]} \\ T_{K/k}/G & \longrightarrow & T^{(1)}_{K/k}, \end{array}$$

where the map in the bottom row is well defined.

Lemma 2.5. *Let $n \geq 3$ be a positive integer. If n is even then the map $[n]$ is not a compression of ϕ, while the map $[n]$ is a compression of ϕ for odd n.*

Proof. Indeed, the map $\Delta_{K/k}$ is G-equivariant if and only if n is odd. □

Remark. If we suppose that k contains ω_n^- instead of ω_n^+, then the torus $T_{k_n/k}$ still contains the cyclic group C_n, but the norm torus $T^{(1)}_{k_n/k}$ does not contain it in general.

3. Galois Cohomology

The aim of this section is to provide some (Galois) cohomological invariants which will be used to get the essential dimension of those groups in Definition 2.2 and to derive generic properties of certain cyclic extensions.

3.1. **Classifying spaces.** Keeping the notation of the previous section we start this section with the following two lemma under the light of Lemma 2.5.

Lemma 3.1. *If n is an odd integer, then there is a canonical isomorphism*

$$H^1(k, G) \cong T^{(1)}_{K/k}(k)/T^{(1)}_{K/k}(k)^n.$$

Proof. The exact sequence (4) gives the long exact cohomology sequence

$$T^{(1)}_{K/k}(k) \xrightarrow{[n]} T^{(1)}_{K/k}(k) \xrightarrow{\delta_k} H^1(k, G) \longrightarrow H^1(k, T^{(1)}_{K/k}) \longrightarrow H^1(k, T^{(1)}_{K/k}).$$

Since n is odd, the n-power map from $k^\times/N_{K/k}K^\times$ to itself is injective. Therefore δ_K is surjective, because of the canonical isomorphism

$$H^1(k, T^{(1)}_{K/k}) \cong k^\times/N_{K/k}K^\times.$$

This settles the proof. □

Note, however, that the lemma does not hold when n is even. Therefore, we now consider a two-dimensional version of Kummer sequence of G for this case. For every even integer $n \geq 4$, we now define a map

$$\pi_n : T_{K/k} \longrightarrow \mathbb{G}_m \times T^{(1)}_{K/k}$$

to be the morphism given by

$$\pi_n(t) = (N_{K/k}(t), \Delta_{K/k}(t)^{n/2}),\ t \in T_{K/k}(\bar{k}).$$

For even n, we can identify ϕ with π_n because of dimension and state an analogue of the previous lemma.

Lemma 3.2. *If $n \geq 4$ is an even integer, then we have the following isomorphism induced by the map π_n:*

$$H^1(K, G) \cong (\mathbb{G}_m \times T^{(1)}_{K/k})(k)/\pi_n T_{K/k}(k).$$

Proof. As in the proof of Lemma 2.4 we can see that G is the kernel of π_n. Moreover there is an exact sequence of Γ_k-modules induced by π_n:

$$1 \to G \to T_{K/k}(\bar{k}) \xrightarrow{\pi_n} (\mathbb{G}_m \times T^{(1)}_{K/k})(\bar{k}) \to 1.$$

Our lemma therefore follows by applying the Galois cohomology to the above sequence, because of vanishing of the first cohomology for the torus $T_{K/k}$. □

3.2. **Cohomological invariants.** For a fixed integer $n \geq 3$, by Lemma 2.4, we have the res map which is given by

$$res : H^1(k, G) \to H^1(k, Res_{K/k}(\mu_n)).$$

From Lemma 3.1 and Lemma 3.2, we have the surjective homomorphism

$$\begin{cases} \delta_k : T^{(1)}_{K/k}(k) \to H^1(k, G), \text{ if } n \text{ odd} \\ \delta_k : k^\times \times T^{(1)}_{K/k}(k) \to H^1(k, G), \text{ if } n \text{ even} \end{cases} \tag{5}$$

which gives a classifying space of the functor $H^1(\ , G)$ over k. For the map res, we have the following formulas.

Proposition 3.3. *Let n be a positive integer. If n is odd, then one has for $\lambda \in T^{(1)}_{K/k}(k)$:*

$$res(\delta_k(\lambda)) = \big[\lambda\big].$$

If $n \geq 4$ is even, then one has for $a \in k^\times$ and $\lambda \in T^{(1)}_{K/k}(k)$:

$$res(\delta_k(a, \lambda)) = \big[a^{n/2}\lambda\big].$$

Here, $[\cdot]$ denotes an equivalence class in $K^\times$ modulo $(K^\times)^n$.

Proof. For our purpose, it suffices to consider the following commutative diagram of Γ_k-modules

$$\begin{array}{ccc} T_{K/k}(\bar{k}) & \xrightarrow{\pi_n} & \mathbb{G}_m(\bar{k}) \times T^{(1)}_{K/k}(\bar{k}) \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \Phi_n} \\ T_{K/k}(\bar{k}) & \xrightarrow{[n]} & T_{K/k}(\bar{k}) \end{array}$$

where $[n]$ stands for the n-th power map with kernel $Res_{K/k}(\mu_n)$ and Φ_n is a morphism given by

$$\Phi(a,\lambda) = a^{n/2}\lambda, \text{ for } a \in \mathbb{G}_m(\bar{k}),\ \lambda \in T^{(1)}_{K/k}(\bar{k}).$$

Here $\mathbb{G}_m$ is regarded as the kernel of the morphism $\Delta_{K/k}$. Then we obtain a commutative diagram with exact rows which shows our formula. □

Remark. For each k-rational point λ of $T^{(1)}_{K/k}$, there is a K-rational point ν of $T_{K/k}$ such that $\lambda = \nu/\bar{\nu}$, because of the Hilbert's 90 theorem. Here $\bar{\nu}$ is the conjugate of ν.

Fix a positive integer $n \geq 2$, and let $m > 1$ be a proper divisor of n. Let G_m be the m order subgroup of G. Denote by η_m the map $H^1(k,G) \to H^1(k,G_m)$ induced by the natural surjection $G \to G_m$. Note that G_m is a twisted k-form of μ_m defined by the composition of f_K with the group homomorphism $Aut(\mu_n) \to Aut(\mu_m)$ (usual restriction).

Lemma 3.4. *Let $n \geq 3$ be a positive integer and m be an odd divisor of n. If n is odd then one has for $\lambda \in K^\times$:*

$$\eta_m(\delta_k(\lambda/\bar{\lambda})) = \delta_k(\lambda/\bar{\lambda})$$

If $n \geq 4$ is even and m is an odd divisor of n then one has for $a \in k^\times$ and $\lambda \in K^\times$:

$$\eta_m(\delta_k(a,\lambda/\bar{\lambda})) = \delta_k(\lambda/\bar{\lambda}),$$

and

$$\eta_2(\delta_k(a,\lambda/\bar{\lambda})) = \begin{cases} \big[N_{K/k}(\lambda)\big], & \text{if } n \equiv 0 \pmod 4 \\ \big[aN_{K/k}(\lambda)\big], & \text{if } n \equiv 2 \pmod 4 \end{cases}.$$

Proof. The first formula comes from exact sequences for G and G_m as in (4). The next formula follows from the following commutative diagram, for any odd divisor m of even n, with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \longrightarrow & T_{K/k}(\bar{k}) & \xrightarrow{\pi_n} & \mathbb{G}_m(\bar{k}) \times T^{(1)}_{K/k}(\bar{k}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle (\Delta_{K/k})^{\frac{n}{2m}}} & & \downarrow{\scriptstyle pr_2} & & \\ 1 & \longrightarrow & G_m & \longrightarrow & T^{(1)}_{K/k}(\bar{k}) & \xrightarrow{[m]} & T^{(1)}_{K/k}(\bar{k}) & \longrightarrow & 1. \end{array}$$

To see the last one we need the isomorphism $k^\times \times T^{(1)}_{K/k}(k)/\pi_2(K^\times) \cong k^\times/(k^\times)^2$ and then the formula follows from a commutative diagram induced by π_n, π_2 and the $n/2$-power map. □

4. Essential dimension

In this section we prove that the essential dimension of G (Definition 2.2) is two if $n \geq 4$ is even. Our proof is based on an idea of Rost [18].

4.1. **Versal pairs.** Retain notations in the previous sections. In the next lemma we summarize a versal pair for G coming from Lemma 2.5.

Lemma 4.1. *Let G be a twisted k-group of μ_n coming from a quadratic extension $k(\sqrt{a})/k$. Then*

$$\begin{cases} \delta_{k(t_1)}(\lambda_{t_1}/\bar{\lambda}_{t_1}) \in H^1(k(t_1), G), & \text{if } n \text{ is odd} \\ \delta_{k(t_1,t_2)}(t_2, \lambda_{t_1}/\bar{\lambda}_{t_1}) \in H^1(k(t_1,t_2), G), & \text{if } n \text{ is even,} \end{cases}$$

is a versal element, where $\lambda_{t_1} = 1 + \sqrt{a}t_1$.

Proof. 1. Let n be odd. Lemma 3.1 and Hilbert's Theorem 90 imply that

$$T^{(1)}_{K/k}(k(t_1)) \cong \{\ \lambda/\bar{\lambda}\ :\ \lambda \in K(t_1)^\times\ \}.$$

Hence the generic point $Spec(k(t_1)) \to T^{(1)}_{K/k}$ determines the 1-cocycle $\delta_{k(t_1)}(\lambda_{t_1}/\bar{\lambda}_{t_1})$ which is a versal element for the functor $H^1(\ , G)$.

2. Applying the similar argument as above to the even case, we obtain that the generic point of $\mathbb{G}_m \times T^{(1)}_{K/k}$ corresponds to the cocycle $\delta_{k(t_1,t_2)}(t_2, \lambda_{t_1}/\bar{\lambda}_{t_1})$ which is versal. □

Corollary 4.2. *Let n be a positive integer and k be the base field satisfying our assumption. Then the splitting field of the polynomial*

1. *$P_n(\omega_n^- t_1, 1, 1; T)$ over $k(t_1)$ if n is odd*
2. *$P_n(\omega_n^- t_1, t_2, 1; T)$ over $k(t_1, t_2)$ if n is even,*

is a versal element for the functor $H^1(\ , C_n)$.

Proof. The canonical map *res* (see the section 2) sends $\delta_{k(t_1)}(\lambda_{t_1}/\bar{\lambda}_{t_1})$to the Kummer extension defined by $\lambda_{t_1}/\bar{\lambda}_{t_1}$. Therefore the lemma follows from the construction of $P_n(\omega_n^- t_1, 1, 1; T)$ in the proof of Theorem 5.1. □

4.2. **Essential dimension.** The essential dimension of G over k is the minimum of the transcendence degree of the field of definition for versal pairs. If denote it by $ed_k G$, then

$$ed_k G = \min \operatorname{trdeg}_k K$$

for all K/k such that there exists a versal G-torsor over K.

For convenience we recall the following notion from Rost [17]. Let v be a valuation on K, and $m > 1$ be a positive integer. An element $[x]$ in $K^\times/(K^\times)^m$ is called *unramified* at v if $[x]$ is non-zero in $K_v^\times/(K_v^\times)^m$, under $U_v/(U_v)^m \to K_v^\times/(K_v^\times)^m$, and *ramified* otherwise. Here, U_v is the group of units of v and K_v is its residue field.

We are now ready to state and prove the following our desired result. With this result, one can conclude that each G-torsor in Lemma 4.1 is minimal among all versal G-torsors over k. Furthermore, it follows that it is not possible to reduce the number of parameters of the polynomials in Theorem 5.1.

Theorem 4.3. *Let $n \geq 4$ be an even integer and k be a base field of characteristic not dividing n. Let G be a twisted form of μ_n coming from a quadratic extension of k. Then*

$$ed_k G = 2.$$

Proof. Denote by $k(\sqrt{a})$ be the splitting field of G_n. Then, by Lemma 4.1 we have the versal element

$$\theta_L = \delta_L\big(x \times \frac{1+\sqrt{a}y}{1-\sqrt{a}y}\ \big) \in H^1(L, G_n),$$

where $L = k(x, y)$. It follows from the definition of k-place that $ed_k G = ed_k \theta_L$. Therefore, our goal is to show that θ_L does not come from a subfield K of L containing k such that $\mathrm{trdeg}_k K \leq 1$. Let $\theta_K \in H^1(K, G_n)$ be an element that maps to θ_L under the map $\phi_K : H^1(K, G_n) \to H^1(L, G_n)$, where K/k is a subextension of L/k. By Lemma 4.1, there are $\alpha \in K^\times,\ \beta \in K(\sqrt{a})^\times$ such that

$$\theta_K = \delta_K\big(\alpha \times \beta/\bar{\beta}\big) \in H^1(K, G_n).$$

The prime element x in $L(\sqrt{a})$ defines a valuation of $L(\sqrt{a})$ such that it is trivial on $k(\sqrt{a})(y)$, denote it by v. We also denote by v the restriction of v on L and by v' the restriction on K.

One has that $\phi_{K(\sqrt{a})} \circ res_K(\theta_K) = res_L(\theta_L)$ $(*)$ by the commutative diagram

$$\begin{array}{ccc} H^1\big(K, G_n\big) & \xrightarrow{\phi_K} & H^1\big(L, G_n\big) \\ {\scriptstyle res_K}\big\downarrow & & \big\downarrow{\scriptstyle res_L} \\ H^1\big(K(\sqrt{a}), \mu_n\big) & \xrightarrow[\phi_{K(\sqrt{a})}]{} & H^1\big(L(\sqrt{a}), \mu_n\big) \end{array}$$

The second formula of Proposition 3.5 implies that $res_L(\omega_L)$ is ramified at v. Thus, from $(*)$ follows that v' is non trivial on $K(\sqrt{a})$ and hence v' is non trivial on K.

We first consider the case $n = 4m$. For the invariant η_2, we obtain $[i] \circ \eta_2\big(\theta_K\big) = \eta_2(\theta_L)$ from the commutative diagram

$$\begin{array}{ccc} H^1\big(K, G_n\big) & \xrightarrow{\phi_K} & H^1\big(L, G_n\big) \\ {\scriptstyle \eta_2}\big\downarrow & & \big\downarrow{\scriptstyle \eta_2} \\ H^1\big(K, \mu_2\big) & \xrightarrow[[i]]{} & H^1\big(L, \mu_2\big). \end{array}$$

Therefore, there is a non zero $f(x, y)$ in L such that

$$N_{K(\sqrt{a})/K}(\beta) = (1 - ay^2) f^2(x, y).$$

Since $(1 - ay^2)$ is not in $(L^\times)^2$, we can conclude that $\mathrm{trdeg}_k\big(k(N_{K(\sqrt{a})/K}(\beta))\big) = 1$. Since $\eta_2(\theta_L)$ is unramified at v, the element $\eta_2(\theta_L)$ is also unramified at v'. Hence the element $N_{K(\sqrt{a})/K}(\beta)$ is in the residue field with respect to the valuation v'. Because v' is nontrivial on K and its residue field contains $k(N_{K(\sqrt{a})/K}(\beta))$, we get the desired result.

Assume $n = 2m$ with $m > 1$ odd. Then the idea is the same as above. We use the invariant η_m instead of η_2, *i.e*, the element

$$\eta_m(\theta_L) = \frac{1-\sqrt{a}y}{1+\sqrt{a}y}$$

is unramified at v. Therefore, we can conclude that $\beta/\bar{\beta}$ is in the residue field with respect to the valuation v' on $K(\sqrt{a})$ because of $\eta_m(\theta_L) \notin (L(\sqrt{a})^\times)^m$. Since v' is non-trivial on $K(\sqrt{a})$, we have $\mathrm{trdeg}_k K(\sqrt{a}) \geq 2$ and hence $\mathrm{trdeg}_k K \geq 2$. This completes the proof. □

Remark. Note that the case $n = 4m$ is a direct consequence of the result of Rost [18]. If the reminder of n by 4 is 2, by Lemma 3.4, then the element $\eta_2(\omega_L)$ is ramified at v.

5. Generic property

This section discusses more specific aspects of the versal torsor corresponding to the group C_n coming from the quadratic extension k_n/k. Here our assumption is that the base field k contains ω_n^+ but does not ζ_n and the characteristic of k is prime to $2n$. The book Jensen-Ledet-Yui [6] is our main reference for this section.

5.1. **Generic polynomial for C_n.** We follow the definition of the generic polynomial for a finite group G over a field k from [6]. A typical example is the polynomial $X^n - t_1 \in k(t_1)[X]$ which parameterizes all C_n extensions over any field containing k if the base field k contains ζ_n and the characteristic of k is prime to n. This is a classical result of Kummer.

The generic dimension of G over a k, denoted by gd_kG, is defined to be the minimal number of parameters in a generic polynomial. Since the essential dimension is a lower bound of the generic dimension, it is desirable to have generic polynomials for C_n over k with ed_kC_n parameters.

Theorem 5.1. *Let $n \geq 3$ be a positive integer, and let k be a field whose characteristic prime to $2n$. If the base field k contains ω_n^+ then*

1. the polynomial

$$P_n(\omega_n^- t_1, t_2, 1; X) \in k(t_1, t_2)[X]$$

is a generic polynomial for the group C_n over k if n is even. In particular, $gd_kC_n = 2$.

2. the polynomial

$$P_n(\omega_n^- t_1, 1, 1; X) \in k(t_1)[X]$$

is a generic polynomial for the group C_n over k if n is odd. In particular, $gd_kC_n = 1$.

Proof. The proof consists of two parts; first, the construction of the polynomial, and second, the proof of the generic property.

Construction. 1. Denote by F the splitting field of $P_n(\omega_n^- t_1, t_2, 1; X)$ over K by putting $K = k(t_1, t_2)$. We claim that F/K is a cyclic Galois extension. Let u be a root of the polynomial $X^n - t_2^{\frac{n}{2}}(1 + t_1\omega_n^-)/(1 - t_1\omega_n^-)$. Then we have a Kummer extension $K_n(u)/K_n$ and now define automorphisms σ and τ on $K_n(u)$ by

σ sends u to $\zeta_n u$ and K_n-linear,

τ sends u to t_2/u and $K_n -$ semilinear over K.

One checks easily that $\sigma, \tau \in \mathrm{Aut}_K(K_n(u))$ and $\sigma^n = \tau^2 = \tau\sigma\tau\sigma^{-1} = id$. Moreover, since τ sends ζ_n to ζ_n^{-1}, we see that

$$\zeta_n^i u + t_2/\zeta_n^i u \in F \text{ for each } i \in \{1, ..., n\},$$

where F stands the fixed part $K_n(u)^\tau$ of τ in $K_n(u)$. For the automorphism σ, one has

$$\sigma^j(\zeta_n^i u + t_2/\zeta_n^i u) = \zeta_n^{i+j} u + t_2/\zeta_n^{i+j} u \tag{6}$$

for any $i, j \in \{1, ..., n\}$. Since $K_n(u)/K_n$ is a cyclic extension of fields, the extension $K_n(u^2)$ is the unique subextension of index 2 in $K_n(u)$ and thus it is different from $K_n(u + t_2/u)$. Therefore $K_n(u) = K_n(u + t_2/u)$ and hence $F = K(u + t_2/u)$ since $[K_n(u) : F] = 2$. Proposition 2.1 tells that

$$P_n(\omega_n^- t_1, t_2, 1; X) = \prod_i \left(X - u\zeta_n^i - \frac{t_2}{u\zeta_n^i} \right) \in K[X].$$

We know that all roots of the polynomial belong to F and hence F/K is a cyclic Galois extension by (6).

2. In this case, we set $K = k(t_1)$ and consider the Kummer extension $K_n(u)/K_n$ with $u^n = (1 + t_1\omega_n^-)/(1 - t_1\omega_n^-)$. Then the same argument in the previous case applies here and hence the splitting field of $P_n(\omega_n^- t_1, 1, 1; X)$ over K is a cyclic Galois. □

Generic property. 2. We need two lemmas for generic property of the polynomial in this theorem. From the following lemma, it follows that the polynomial constructed above for odd n is still generic for any n if we require that k contains ζ_n.

Lemma 5.2. *Let F/K be a Galois C_n-extension of fields over k. Assume $\zeta_n \in F$. Then F is the splitting field of the polynomial $P_n(\omega_n^- b, a, 1; t) \in K[X]$ for some $a, b \in K^\times$.*

Proof. We distinguish two cases.

A) Assume $\zeta_n \in K$. Then F is of the form $K(u)$ where $u^n = c$ for some $c \in K^\times$, by Kummer's theorem. Note here that $c \neq \pm 1$, because $n > 2$. Since $[K(u) : K(u+u^{-1})] \leq 2$, one has $K(u) = K(u + u^{-1})$. In fact, if n is even, then $K(u^2)$ is the unique subextension of index 2 in $K(u)$, which does not contain $u + u^{-1}$. Hence we choose $a = 1$ and $b = (1 - c)/(1 + c)\omega_n^- \in K^\times$.

B) Assume $\zeta_n \notin K$. Then n is even. Denote by σ the generator of the Galois group of F/K. Then there is $u \in F$ such that $u^m = c \in K_n \setminus K$ and $\sigma^2(u) = u\zeta_n^2$, where $m = n/2$. Writing $v = \sigma(u)$, we deduce that $uv\zeta_n$ is fixed by σ and so $uv\zeta_n \in K^\times$. Denote it by b and consider the image of c^2/b^m under the norm map $N_{K_n/K}$. Then $N_{K_n/K}(c^2/b^m) = 1$. By Hilbert's 90 theorem, one has $u^n = b^m(1 + \omega_n^- a)/(1 - \omega_n^- a)$ for some $a \in K^\times$. Observing that all roots of the polynomial $P_n(\omega_n^- a, b, 1; X)$ belong to F and for any integer j

$$\sigma^j(u + b/u) = u\zeta_n^j + b/u\zeta_n^j,$$

we conclude that $F = K(u + b/u)$ by Galois's fundamental theorem. □

Example. Let $K = \mathbb{F}_7$. Set $E = K(\sqrt{2\sqrt{-1} - 1})$. Then F/K is a C_4 extension containing the quadratic extension $K(\sqrt{-1})/K$.

Lemma 5.3. *Let F/K be as in the previous lemma. Assume that $\zeta_n \notin F$. Then F is the splitting field of the polynomial $P_n(\omega_n^- b, a, 1; X) \in K[X]$ for some $a, b \in K^\times$. Moreover, we may choose $a = 1$ for odd n.*

Proof. The cohomology group $H^1(K, C_n)$ classifies the Galois C_n-algebras over K up to isomorphism. Let $[F] \in H^1(K, C_n)$ be the class corresponding to the C_n-extension F/K.

If n is even, then there are $a \in K^\times$ and $\lambda \in K_n^\times$ such that the pair (a, λ) maps to F/K under δ_K by (5). Using Proposition 3.3 and its remark we can deduce that there is $c + \omega_n^- b \in K_n^\times$ so that

$$res_K([F]) = \Big[\ a^{n/2}\frac{c + \omega_n^- b}{c - \omega_n^- b}\ \Big].$$

Since $\zeta_n \notin F$ we have a field $F \otimes_K K_n$, and denote it by E. Thus the above formula imply that $bc \neq 0$, and hence we may assume that $c = 1$. So we can choose an element $u \in E$ such that $u^n = a^{n/2}\frac{1+\omega_n^- b}{1-\omega_n^- b} \in K_n$ and $\sigma(u) = u\zeta_n$, where σ generates the Galois group of E/K_n. Define an K_n-semilinear automorphism $\tau : E \to E$ over K by $\tau(u) = a/u$. By

Galois descent with respect to K_n/K, the field F is the fixed part of τ in E. Moreover, we have $\sigma\tau = \tau\sigma$ and

$$u\zeta_n^i + a\zeta_n^{-i}/u \in F \text{ for each } i \in \{1, 2, ..., n\}.$$

We now claim that $E = K_n(u+a/u)$. Since E/K_n is a C_n-extension of fields, the extension $K_n(u^2)$ is the unique subextension of $K_n(u)$ of degree $n/2$ over K_n. The claim then follows from $[E : K_n(u+a/u)] \leq 2$ and a fact that $K_n(u^2) = K_n(u+a/u)$ is impossible. Therefore $[E : K(u + a/u)] = 2$ and hence F is as required.

If n is odd, then Lemma 3.1 and Hilbert's Theorem 90 imply that there is $b, c \in K$ such that

$$res_K([F]) = \left[\frac{c + \omega_n^- b}{c - \omega_n^- b}\right].$$

By applying an argument similar to the previous case, we can finish the proof of the lemma. □

Remark. Lenstra's theorem states that generic polynomials exist for a finite abelian group G over $\mathbb{Q}$ if and only if G has no elements of order 8. However, Theorem 5.1 says that there is a generic polynomial for any group C_{8m} over $\mathbb{Q}(\omega_{8m}^+)$.

Corollary 5.4. *Let n be a positive integer and k be a field of characteristic not dividing $2n$. Assume $\omega_n^+ \in k$ but $\zeta_n \notin k$. Then*

$$ed_k C_n = gd_k C_n = \begin{cases} 1, & \text{if } n \text{ is odd} \\ 2, & \text{if } n \text{ is even} \end{cases}$$

where $ed_k C_n$ denotes the essential dimension for C_n over k.

Proof. The statement for the generic dimension of C_n follows from a lower bound in Lemma 4.3 and an upper bound provided by the number of parameters of our polynomials. For odd n, Lemma 4.1.1 implies that $ed_k C_n \leq 1$ and thus $ed_k C_n = 1$, since $ed_{k_n}\mu_n = 1$. □

5.2. **Descent Generic Cyclic Polynomials.** Kemper [7] proved that every generic polynomial for a finite group G over a field K is descent-generic when the field L above is permitted to be an infinite field. We now discuss descent generic property of the polynomial in the Theorem 5.1, *i.e*, we ant to show the following stronger property:

For each subgroup C_m of C_n, every extension N/L with Galois group C_m can be obtained as the splitting field of a polynomial which is the specialization of $P(X)$ resulting from setting the indeterminate variables to elements of L. Here $P(X)$ denotes the polynomial introduced in Theorem 5.1.

Lemma 5.5. *Let $m > 2$ be a divisor of an integer n. If ω_n^+, $\zeta_m \in k$ then $\zeta_n \in k$.*

Proof. Assume $\zeta_n \notin k$. Since $\omega_n^+ \in k$ then the Galois group of the extension k_n/k consists of id and τ, where $\tau(\zeta_n) = \zeta_n^{-1}$. It must be $\tau(\zeta_m) = \zeta_m$ and $\zeta_m = \zeta_m^{-1}$ because of $\zeta_m \in k$ and $m|n$. This implies $m = 2$ which is a contradiction. □

Proposition 5.6. *The generic polynomials introduced in Theorem 5.1 are descent generic.*

Proof. Assume $m \geq 1$ is a divisor of odd n. Obviously $\omega_m^+ \in k$. Now consider an extension N/L with Galois group C_m. We have seen that there is $a \in L^\times$ such that the extension $[N/L]$ is defined by $\delta_L\big((1+\omega_m^- a)/(1-\omega_m^- a)\ \big)$. Since $L_m \subset L_n$, we have the following expression

$$(1 \pm \omega_m^- a)^{n/m} = A \pm \omega_n^- B \text{ for some } A, B \in L^\times.$$

Thus we claim that N is the splitting field of $P_n(\omega_n^- B/A, 1, 1; T)$ over L. Indeed, this polynomial is equal to the product

$$\prod_{i=1}^{n} \left(T - u\zeta_n^i - 1/u\zeta_n^i\right),$$

where u satisfies the relation $u^m = (1+\omega_m^- a)/(1-\omega_m^- a)$. Because of the previous lemma, the field $L_m(u)$ contains $u\zeta_n^i + a/\zeta_n^i u$ for each $i \leq n$. Note that Lemma 3.4 imply $res_L([N/L]) = [L_m(u)/L_m]$, and furthermore $N = L_m(u)^\tau$ for an automorphism τ on $L_m(u)$ defined as in the proof of Theorem 5.1.

A similar argument works in the even case. □

Remark. The proof of Proposition 5.6 is based on the following commutative diagram:

$$\begin{array}{ccc} H^1\big(L, C_m\big) & \longrightarrow & H^1\big(L, C_n\big) \\ {\scriptstyle res_L}\big\downarrow & & \big\downarrow{\scriptstyle res_L} \\ H^1\big(L_m, \mu_m\big) & \longrightarrow & H^1\big(L_n, \mu_n\big). \end{array}$$

which is induced by the natural inclusion $C_m \to C_n$. For example, in the proof above, the 1-cocycle $res_L(\delta_L(\lambda)) \in H^1\big(L_n, \mu_n\big)$ determines the Kummer extension $L_n(v)/L_n$ with $v^n = \lambda$, where $\lambda = (A + \omega_n^- B)/(A - \omega_n^- B)$.

5.3. **Generic Cyclic Extensions.** Ledet [10] proved that the existence of a generic polynomial for a group G over an infinite field K is equivalent to the existence of a generic extension of G over K. In order to compare the generic polynomials in Theorem 5.1, we now construct an explicit family of generic cyclic Galois extension over the base field k.

Let us recall the definition of generic Galois extensions introduced by Saltman in [19]. We should mention that generic cyclic extensions are also discussed in his paper.

Definition 5.7. *A Galois extension S/R with group G is called a generic G-extension over k, if*

1. R is of the form $k[t_1, ...t_m, 1/t]$ for some $t \in k[t_1, ..., t_m]^\times$, and

2. whenever K is an extension field of k and F/K is a Galois algebra with group G, there is a k-algebra homomorphism $\phi : R \to K$, such that $S \otimes_\phi K/K$ and F/K are isomorphic as Galois extensions.

Let k have characteristic prime to n and assume $\zeta_n \in k$. Denote by S the commutative ring $R[X]/(X^n - t)$, where R is the localized polynomial ring $k[t, 1/t]$. Then the extension S/R is generic for C_n over k. We recall the following result which is Proposition 0,6 (a) in [19].

Lemma 5.8. *Let n prime to the characteristic of k and assume $\zeta_n \in k$. If a is a unit of R, and $S = R[x]/(x^n - a)$, then S/R is Galois with group C_n. Then the action of C_n on S is defined by $\sigma(\alpha) = \alpha\zeta_n$, where α is a canonical generator of S, and σ generates C_n.*

From now on, we may assume that the base field does not contain ζ_n.

Proposition 5.9. *Let $n \geq 3$ be a positive integer and k be a field of characteristic prime to $2n$. Assume k contains ω_n^+. Then S/R is a cyclic Galois extension of k-algebras. Here, if n is even, then*

$$R = k\big[x, y, z, 1/y(z^2 - (\omega_n^+ - 4)x^2)\big] \text{ and } S = R[T]/\langle P_n(\omega_n^- x, y, z; T)\rangle,$$

If n is odd, then

$$R = k\big[x, z, 1/(z^2 - (\omega_n^+ - 4)x^2)\big] \text{ and } S = R[T]/\langle P_n(\omega_n^- x, 1, z; T)\rangle.$$

Proof. Assume n is even and set $a = y^{n/2}(z + \omega_n^- x)/(z - \omega_n^- x)$. Then a is a unit of $R_n = R \otimes_k k_n$. On applying Lemma 5.8 to a, we obtain a C_n-extension $R_n[u]/R_n$ such that $u^n = a$ and the C_n-action on $R_n[u]$ is defined by $\sigma(u) = u\zeta_n$ for a fixed generator σ of C_n. Consider an R-linear C_2-action on $R_n[u]$ given by

$$\tau(u) = y/u \quad \text{and} \quad \tau(\zeta_n) = \zeta_n^{-1}$$

for the generator τ in C_2. Then clearly τ commutes with σ. Moreover, the extension F/R inherits the C_n-structure from $R_n[u]/R_n$, where F is the fixed part of τ in $R_n[u]$,

In order to show that S is isomorphic with F as a k-algebra, we define a map ϕ from $R[T]$ to F by

$$\phi|_R = id \text{ and } \phi(T) = u + y/u.$$

Theorem 5.1 shows that the polynomial $P_n(\omega_n^- x, y, z; T)$ is irreducible. Thus, ϕ is a well defined k-algebra homomorphism by Lemma 2.1 and is injective. By comparing dimensions over R we can see that $S \cong F$ via the homomorphism ϕ. Therefore, S/R is a Galois C_n-extension.

Let F/K be a Galois C_n-algebra with K a field. Then there are non zero $a \in K$ and $\nu \in K_n$ such that $\delta_K(a, \nu/\bar{\nu}) = [F/K]$ by (5). Now it is natural to define a map ϕ from R to K by sending y to a and $z + \omega_n^- x$ to ν. We then have that $S \otimes_\phi K \cong F$ as C_n-modules by Proposition 5 and the description of F.

Odd case is similar to the even case above. □

References

[1] G. Bayarmagnai, *Essential dimension of some twists of μ_{p^n}*, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 145-151, RIMS Kôkyûroku Bessatsu, (RIMS), (2007).

[2] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group* Comp. Math. 106, 159-179 (1997).

[3] G. Berhuy, G.Favi, *Essential dimension: a Functorial Point of View (After A. Merkurjev)* Doc. Math. 8, 279-330 (2003).

[4] M. Florence, *On the essential dimension of cyclic p-groups*,Invent. Math. 171 (2008).

[5] S. Garibaldi, A. Merkurjev, J.-P. Serre, *Cohomological invariants in Galois cohomology*, Univ.Lecture Ser, vol. 28, Amer. Math. Soc., Providence, RI, (2003).

[6] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications, Cambridge. University Press (2002).

[7] G. Kemper, *Generic polynomials are descent-generic,* Manuscripta Math. 105 139-141 (2001).

[8] M. A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions*, AMS Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, (1998).

[9] K. Hashimoto, Y. Rikuna, *On generic families of cyclic polynomials with even degree*, Manuscripta Math. 107, 283-288 (2002).

[10] A. Ledet, *Generic Extensions and Generic Polynomials*, J. Symbolic Comput. 30 , 867-872 (2000).
[11] H. W. Jr. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. 25, 299-325 (1974).
[12] R. Lötscher, A. Meyer, M. MacDonald, Z. Reichstein, *Essential p-dimension of algebraic tori*, Preprint October (2009).
[13] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer-Verlag, Berlin, (1999).
[14] Z. Reichstein, *On the notion of essential dimension for algebraic groups* , Transformation Groups, no 3, 265-304 (2000).
[15] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation Groups 5, no. 3, 265-304 (2000).
[16] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. 130, 2215-2218 (2002).
[17] M. Rost, *Computation of some essential dimensions*, (2000). Available on http://www.math.ohio-state.edu/rost/ed.html
[18] M. Rost, *Essential dimension of twisted C_4*, (2000).
[19] D. J. Saltman, *Generic Galois Extensions and Problems in Field Theory* , Adv. in Math. 43, 250-283 (1982).
[20] D. J. Saltman, *Retract rational fields and cyclic Galois extensions* Israel J. Math. 47, 165-215 (1984).
[21] J.-P. Serre, *Galois Cohomology*, Heidelberg: Springer-Verlag, (1997).
[22] G. W. Smith, *Generic cyclic polynomials of odd degree*, Comm. Algebra, 19, no. 12, 3367-3391 (1991).

E-mail address: gbayarmagnai@yahoo.com